UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/767,292	01/18/2001	Arthur Doskow	414.038CIP/10007256	9811

32127	7590	05/31/2006

VERIZON CORPORATE SERVICES GROUP INC.
C/O CHRISTIAN R. ANDERSEN
600 HIDDEN RIDGE DRIVE
MAILCODE HQEO3H14
IRVING, TX 75038

EXAMINER
KLIMACH, PAULA W

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 05/31/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<table>
<tr><td rowspan="3">Office Action Summary</td><td>Application No.
09/767,292</td><td>Applicant(s)
DOSKOW ET AL.</td></tr>
<tr><td>Examiner
Paula W. Klimach</td><td>Art Unit
2135</td></tr>
</table>

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>*07 February 2006*</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-38* is/are pending in the application.

  4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

  Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

  Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

  a)☐ All b)☐ Some * c)☐ None of:

   1.☐ Certified copies of the priority documents have been received.

   2.☐ Certified copies of the priority documents have been received in Application No. _____.

   3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

  * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
  Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
  Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in

37 CFR 1.17(e), was filed in this application after final rejection. Since this application is

eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e)

has been timely paid, the finality of the previous Office action has been withdrawn pursuant to

37 CFR 1.114. Applicant's submission filed on 03/03/06 has been entered.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1 and 5-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over

applicant admitted prior art in view of Bissell et al (6,574,730) and further in view of the book by

Schneier ("Applied Cryptography").

In reference to claim 1, applicant admitted prior art discloses system local

communication links that include a plurality of separately located central office switching system

inter connected via trunk circuits for selectively providing switched call connection links in

response to predetermined control data messages (page 5 lines 25-30). The applicant admitted

prior art discloses the use of the SS7 network (page 6 lines 5-10). In that case the plurality of

central office switching systems would be enabled to talk to each other using a singling

communication system for two-way communications of said control data messages between the

central office switching system, said signaling communication system interconnecting the central

office switching systems (page 6 lines 1-5). Regarding the signaling gateway, separate from the

central office switching systems and connected to said signaling communications system, said

signaling gateway including an interface connected to a remote communications said remote

communication network and said signaling communication system (page 5 line 25 to page 6 line

17).

   Although applicant discloses, in applicant admitted prior art (page 5-6), sending

messages securely on the network using a gateway to filter messages, the admitted prior art does

not disclose the signaling system security monitor configured to evaluate an encrypted portion of

said control data messages so as to authenticate corresponding ones of said control messages

and, in response, determine if said control data messages are proper.

   Bissell discloses a signaling system security monitor (security node) that is separate from

the central office switching system (local exchange) (column 6 lines 33-45). The security node

is configured to evaluate an encrypted portion of said control data messages (authentication

code) so as to authenticate the message (column 5 lines 15-65 in combination with column 6

lines 28-33).

   At the time the invention was made, it would have been obvious to a person of ordinary

skill in the art to authenticate the messages as in Bissell in the system of the admitted prior art.

One of ordinary skill in the art would have been motivated to do this because the system would

remove the call set-up procedure carried out by the customer, which would remove the
inconvenience from the customer.

Bissell does not expressly disclose a control data message that includes digital time
stamps, wherein the control data message is proper including timely and properly sequenced.

Schneier discloses a message that Alice constructs where T_A is a timestamp (page 576).
The system disclosed by Schneier utilizes the timestamp to confirm the message is current and
therefore properly sequenced.

At the time the invention was made, it would have been obvious to a person of ordinary
skill in the art to utilize the timestamp with the messages as created in the system disclosed by
Schneier in the system of Bissell. One of ordinary skill in the art would have been motivated to
do this because the timestamp may be used to determine whether there has been fraud by the
reuse of a message that is sent out of sequence (Schneier page 38).

In reference to claim 5, wherein said signaling system security monitor is configured to
selectively communicate said control data messages between said signaling gateway and said
signaling communication system in response to said encrypted portions of said control data
messages.

Bissell discloses a system wherein the messages are selectively communicated in
response to the encrypted portions of the control data messages (authentication code). The
customer call is only allowed to proceed in the normal way if the authentication process is
positive (column 5 line 65 to column 6 line 12).

At the time the invention was made, it would have been obvious to a person of ordinary
skill in the art to authenticate the messages as in Bissell in the system of as discloses by the

applicant prior art. One of ordinary skill in the art would have been motivated to do this because the system would remove the call set-up procedure carried out by the customer, which would remove the inconvenience form the customer.

In reference to claim 6, wherein said signaling system security monitor is configured to selectively enable and inhibit said signaling gateway from exchanging said control data messages between said remote communication network and said signaling communication system in response to said encrypted portions of said control data messages.

Bissell discloses a system wherein the messages are selectively communicated in response to the encrypted portions of the control data messages (authentication code). The customer call is only allowed to proceed in the normal way if the authentication process is positive (column 5 line 65 to column 6 line 12). Bissell also discloses inhibiting the communication after a number of attempts (column 6 lines 28-33).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to authenticate the messages as in Bissell in the system as disclosed by applicant admitted prior art. One of ordinary skill in the art would have been motivated to do this because the system would remove the call set-up procedure carried out by the customer, which would remove the inconvenience form the customer.

In reference to claim 7, wherein said signaling system security monitor includes a memory storing states of respective ones of said central office switching system, said processor additionally responsive to said states for determining if said control messages are proper.

Applicant admitted prior art does not expressly disclose using states to determine if the control messages are proper.

Bissell discloses operation of a telephony service may be modeled in terms of a sequence of states a call may go through. Bissell uses the off-hook condition to define when and how authentication is initiated (column 8 lines 9-50); and therefore when the control messages are proper.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the call model as in Bissell in the system as disclosed by applicant admitted prior art. One of ordinary skill in the art would have been motivated to do this because this would provide a means to know when an error has occurred.

In reference to claim 8, the gateway is configured to convert form SS7 type message to another packet data format, IP packets for the Internet (page 6 lines 10-17).

In reference to claim 9, the other packet data format is IP format (page 6 lines 12).

In reference to claim 10, the applicant admitted prior art does not disclose the security monitor configured to monitor a destination point, originating point pr service indicator.

Bissell discloses regarding the security monitor configured to monitor at least one of (i) a destination point code, (ii) an originating point code, and (iii) a service indicator (column 5 line 65 to column 6 line 12).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to authenticate the messages as in Bissell in the system as disclosed in applicant admitted prior art. One of ordinary skill in the art would have been motivated to do this because the system would remove the call set-up procedure carried out by the customer, which would remove the inconvenience form the customer.

In reference to claim 11, wherein said signaling system monitor is configured to monitor at least one of SCCP, ISUP, TCAP, and AIN messages (page 6 lines 1-15).

In reference to claim 12, wherein said signaling system security monitor is configured to monitor calling and called party address parameters contained in SCCP message portions of said control data messages and determine if said monitor calling and called party address parameter are consistent with an authorized signaling relationship (page 6 lines 18-29).

In reference to claim 13, wherein said signaling system security monitor is configured to monitor calling and called party address parameters contained in an SCCP message portion of said control data message (page 6 lines 18-29).

In reference to claim 14, wherein said signaling system security monitor is configured to monitor origination and designation point codes and calling and called party address parameters contained in a TCAP message portion of said control data messages.

Bissell discloses regarding the security monitor configured to monitor at least one of (i) a destination point code, (ii) an originating point code, and (iii) a service indicator (column 5 line 65 to column 6 line 12).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to authenticate the messages as in Bissell in the system as disclosed in the applicant admitted prior art. One of ordinary skill in the art would have been motivated to do this because the system would remove the call set-up procedure carried out by the customer, which would remove the inconvenience form the customer.

In reference to claim 15, applicant admitted prior art does not disclose a system of wherein party address parameters contained in a TCAP message portion of said control data messages.

Bissell discloses a system wherein said signaling system security monitor is configured to monitor origination and designation point codes and calling and called party address parameters contained in a TCAP message portion of said control data messages (column 5 line 65 to column 6 line 12).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to authenticate the messages as in Bissell in the system as disclosed in the applicant admitted prior art. One of ordinary skill in the art would have been motivated to do this because the system would remove the call set-up procedure carried out by the customer, which would remove the inconvenience form the customer.

In reference to claim 16, wherein said signaling system security monitor includes a memory storing state of communication network.

Applicant admitted prior art does not expressly disclose storing states of the communication network.

Bissell discloses operation of a telephony service may be modeled in terms of a sequence of states a call may go through. Bissell uses the off-hook condition to define when and how authentication is initiated (column 8 lines 9-50); and therefore when the control messages are proper. The states would have to be stored for the authentication process to know what to send next.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the call model as in Bissell in the system as disclosed in applicant admitted prior art. One of ordinary skill in the art would have been motivated to do this because this would provide a means to know when an error has occurred.

In reference to claim 17, wherein said signaling system security monitor includes a memory storing permissible states of said communications network and rules for transitioning form each of said permissible states to others of said permissible states.

Applicant admitted prior art expressly disclose storing states of the communication network.

Bissell discloses operation of a telephony service may be modeled in terms of a sequence of states a call may go through. Bissell uses the off-hook condition to define when and how authentication is initiated (column 8 lines 9-50); and therefore when the control messages are proper. The states would have to be stored for the authentication process to know what to send next. The steps taken for the authentication to be positive imply the rules for transition from one state to another.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the call model as in Bissell in the system as disclosed by applicant admitted prior art. One of ordinary skill in the art would have been motivated to do this because this would provide a means to know when an error has occurred.

Claims 2-3 are rejected under 35 U.S.C. 103(a) as being unpatentable over applicant admitted prior art and Bissell and further in view of the book by Schneier ("Applied Cryptography") as applied to claim 1 above, and further in view of Sawyer et al (6,324,271 B1).

In reference to claim 2, Bissell does not disclose a system wherein the security monitor comprises a certification agent configured to exchange and maintain encryption key certificates.

Sawyer discloses an authentication server on an SS7 network (Fig. 1 part 80) that is configured to exchange and maintain encryption key certificates (column 5 lines 27-33). Sawyer teaches that the system uses the X.509 protocol. The X.509 is a digital certificate that is distributed in order to authenticate the user.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use digital certificates as in Sawyer in the system as disclosed in applicant admitted prior art. One of ordinary skill in the art would have been motivated to do this because digital certificates assert that the specific token is linked to a unique person at a specific time and date.

In reference to claim 3, wherein the signaling system security monitor is configured to issue and decrypt digital time stamps.

Bissell do not disclose the use of digital time stamps.

Sawyer discloses the use of digitally signed time-stamp (column 5 lines 40-47).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use digital time-stamps as in the system of Sawyer in the system as disclosed in applicant admitted prior art. One of ordinary skill in the art would have been motivated to do this because it would protect against certificate replay.

Claims 4 are rejected under 35 U.S.C. 103(a) as being unpatentable over applicant

admitted prior art and Bissell and further in view of the book by Schneier ("Applied

Cryptography") as applied to claim 1 above, and further in view of Arkko et al (20020052200

A1).

In reference to claim 4, Bissell do not disclose the use of a digital certificate issuing

authority.

Arrko discloses the use of a Key Administration center that performs the duties of a

digital certificate issuing authority on an SS7 Network (page 3 paragraphs 0035-0037).

At the time the invention was made, it would have been obvious to a person of ordinary

skill in the art to use digital certificate issuing authority as disclosed by Arrko in the system as

disclosed in applicant admitted prior art. One of ordinary skill in the art would have been

motivated to do this because certificate authorities provide assurance of the identity of the key

holder and therefore increase the security of the system.

Claims 18-24 rejected under 35 U.S.C. 103(a) as being unpatentable over applicant

admitted prior art and Bissell and further in view of the book by Schneier ("Applied

Cryptography") as applied to claim 1 above, and further in view of Hanson et al (6,014,427).

In reference to claim 18, wherein said signaling system security monitor includes a

memory storing data relating call progress status with respective sets of control messages

appropriate to initiate a next action consistent with a particular service.

Bissell does not storing data relating call progress status with respective sets of control

messages appropriate to initiate a next action consistent with a particular service.

Hanson discloses a voice mail messaging system wherein the system stores messages

depending on the progress of the call (Fig. 4). The user can prompt the caller so as to initiate a

next action, the action would lead to the service associated with the prompt (column 4 lines 40-

50).

At the time the invention was made, it would have been obvious to a person of ordinary

skill in the art to relate cal progress status with the respective sets of control messages as in

Hanson in the system as disclosed by applicant admitted prior art. One of ordinary skill in the art

would have been motivated to do this because the user would be allowed to custom the message

on the system.

In reference to claim 19, wherein the signaling system security monitor includes a

memory storing a plurality of message templates.

Applicant admitted prior art and Bissell do not disclose storing a plurality of message

templates.

However, Hanson discloses a system wherein the user can store a plurality of message

templates (Fig. 4A part 406).

At the time the invention was made, it would have been obvious to a person of ordinary

skill in the art to relate cal progress status with the respective sets of control messages as in

Hanson in the system as disclosed by applicant admitted prior art. One of ordinary skill in the art

would have been motivated to do this because the user would be allowed to custom the message

on the system.

In reference to claim 20, the messages disclosed by Hanson are dependent on the user and therefore the user may refer to a plurality of service providers, wherein each provider is represented by a prompt.

In reference to claim 21, the action messages allow the user to relate a prompt with a message; therefore each service provider would correspond to a message and the caller would chose a prompt as shown in Hanson for the action to be taken.

In reference to claim 22, wherein said signaling system security monitor includes a memory storing sets pf templates, each of said sets corresponding to control messages appropriate to particular call progress flow.

Applicant admitted prior art and Bissell do not storing sets pf templates, each of said sets corresponding to control messages appropriate to particular call progress flow.

Hanson discloses a voice mail messaging system wherein the system stores messages depending on the progress of the call (Fig. 4). The user can prompt the caller so as to initiate a next action, the action would lead to the service associated with the prompt (column 4 lines 40-50). The progress of the call would correspond to the progress flow.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to relate cal progress status with the respective sets of control messages as in Hanson in the system of applicant admitted prior art. One of ordinary skill in the art would have been motivated to do this because the user would be allowed to custom the message on the system.

In reference to claim 23, Applicant admitted prior art discloses a system wherein the message format is AIN and TCAP (column 8 lines 26-39).

In reference to claim 24, the system disclosed by Hanson selects the message templates that relate to the message to play back to the caller in relation to the prompt.

Claims 25-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over applicant admitted prior art in view of Sawyer et al (6,324,271 B1) and further in view of the book by Schneier ("Applied Cryptography").

In reference to claim 25, applicant admitted prior art discloses a method of securely interfacing control links of respective communication networks, comprising the step of exchanging control messages between a remote communication network and a local signaling communication system (Fig. 1).

However applicant admitted prior art does not disclose decrypting a certificate portion of said control messages so as to authenticate origination point code information; selectively communicating, in response to said decrypting step, control data messages between central office switching systems; and selectively providing switched call connections between at least two of the local communication links in response to predetermined control data messages.

Sawyer discloses an authentication server on an SS7 network (Fig. 1 part 80) that is configured to exchange and maintain encryption key certificates (column 5 lines 27-33). Sawyer teaches that the system uses the X.509 protocol. The X.509 is a digital certificate that is distributed in order to authenticate the user. Sawyer discloses a digital signature; digital signatures are decrypted in order to authenticate the signature. This information is used to authenticate the terminal 10; and then therefore selectively provide the connection for the terminal.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use digital certificates as in Sawyer in the system as disclosed in applicant admitted prior art. One of ordinary skill in the art would have been motivated to do this because digital certificates assert that the specific token is linked to a unique person at a specific time and date.

Bissell does not expressly disclose a control data message that includes digital time stamps, wherein the control data message is proper including timely and properly sequenced.

Schneier discloses a message that Alice constructs where T_A is a timestamp (page 576). The system disclosed by Schneier utilizes the timestamp to confirm the message is current and therefore properly sequenced.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize the timestamp with the messages as created in the system disclosed by Schneier in the system of Bissell. One of ordinary skill in the art would have been motivated to do this because the timestamp may be used to determine whether there has been fraud by the reuse of a message that is sent out of sequence (Schneier page 38).

In reference to claim 26, the gateway is configured to convert form SS7 type message, at the local network, to another packet data format, IP packets for the Internet (page 6 lines 10-17).

In reference to claim 27, the messages in the local network are SS7 complain message protocol (page 6 lines 10-17).

In reference to claim 28, the other packet data format is IP format (page 6 lines 12).

In reference to claim 29, wherein said signaling system security monitor is configured to monitor calling and called party address parameters contained in an SCCP message portion of said control data message (page 6 lines 18-29).

In reference to claim 30, wherein said signaling system security monitor is configured to monitor calling and called party address parameters contained in SCCP message portions of said control data messages and determine if said monitor calling and called party address parameter are consistent with an authorized signaling relationship (page 6 lines 18-29).

In reference to claim 31, wherein said signaling system security monitor is configured to monitor origination and designation point codes and calling and called party address parameters contained in a TCAP message portion of said control data messages (column 8 lines 26-50).

Bissell discloses a system wherein said signaling system security monitor is configured to monitor origination and designation point codes and calling and called party address parameters contained in a TCAP message portion of said control data messages (column 5 line 65 to column 6 line 12).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to authenticate the messages as in Bissell in the system as disclosed in the applicant admitted prior art. One of ordinary skill in the art would have been motivated to do this because the system would remove the call set-up procedure carried out by the customer, which would remove the inconvenience form the customer.

In reference to claim 32, wherein said signaling system security monitor is configured to monitor origination and designation point codes and calling and called party address parameters contained in a TCAP message portion of said control data messages.

Bissell discloses a system wherein said signaling system security monitor is configured to

monitor origination and designation point codes and calling and called party address parameters

contained in a TCAP message portion of said control data messages (column 5 line 65 to column

6 line 12).

At the time the invention was made, it would have been obvious to a person of ordinary

skill in the art to authenticate the messages as in Bissell in the system as disclosed in the

applicant admitted prior art. One of ordinary skill in the art would have been motivated to do

this because the system would remove the call set-up procedure carried out by the customer,

which would remove the inconvenience form the customer.

Claim 34 is rejected under 35 U.S.C. 103(a) as being unpatentable over applicant

admitted prior art and Sawyer and further in view of the book by Schneier ("Applied

Cryptography") as applied to claim 25 above, and further in view of Bissell.

In reference to claim 34, wherein said signaling system security monitor includes a

memory storing state of communication network.

Applicant admitted prior art does not expressly disclose storing states of the

communication network.

Bissell discloses operation of a telephony service may be modeled in terms of a sequence

of states a call may go through. Bissell uses the off-hook condition to define when and how

authentication is initiated (column 8 lines 9-50); and therefore when the control messages are

proper. The states would have to be stored for the authentication process to know what to send

next.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the call model as in Bissell in the system as disclosed in applicant admitted prior art. One of ordinary skill in the art would have been motivated to do this because this would provide a means to know when an error has occurred.

Claims 35-38 rejected under 35 U.S.C. 103(a) as being unpatentable over applicant admitted prior art and Sawyer and further in view of the book by Schneier ("Applied Cryptography") as applied to claim 25 above, and further in view of Hanson et al (6,014,427).

In reference to claim 35, wherein said signaling system security monitor includes a memory storing data relating call progress status with respective sets of control messages appropriate to initiate a next action consistent with a particular service.

Applicant admitted prior art and Sawyer do not storing data relating call progress status with respective sets of control messages appropriate to initiate a next action consistent with a particular service.

Hanson discloses a voice mail messaging system wherein the system stores messages depending on the progress of the call (Fig. 4). The user can prompt the caller so as to initiate a next action, the action would lead to the service associated with the prompt (column 4 lines 40-50).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to relate cal progress status with the respective sets of control messages as in Hanson in the system as disclosed by applicant admitted prior art. One of ordinary skill in the art

would have been motivated to do this because the user would be allowed to custom the message

on the system.

In reference to claim 36, wherein the signaling system security monitor includes a

memory storing a plurality of message templates.

Applicant admitted prior art and Bissell do not disclose storing a plurality of message

templates.

However, Hanson discloses a system wherein the user can store a plurality of message

templates (Fig. 4A part 406).

At the time the invention was made, it would have been obvious to a person of ordinary

skill in the art to relate cal progress status with the respective sets of control messages as in

Hanson in the system as disclosed by applicant admitted prior art. One of ordinary skill in the art

would have been motivated to do this because the user would be allowed to custom the message

on the system.

In reference to claim 37, the messages disclosed by Hanson are dependent on the user

and therefore the user may refer to a plurality of service providers, wherein each provider is

represented by a prompt.

In reference to claim 38, the action messages allow the user to relate a prompt with a

message; therefore each service provider would correspond to a message and the caller would

chose a prompt as shown in Hanson for the action to be taken.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK
Thursday, May 11, 2006

HOSUK SONG
PRIMARY EXAMINER